UNITED STATES DISTRICT COURT NORTHERN DISTRICT OF ILLINOIS

DANIELLE RENINGER on behalf of herself and others similarly situated,

Plaintiff,

v.

FACEBOOK, INC.,

Defendant.

CASE NO.

CONSUMER CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

I. INTRODUCTION

1. Plaintiff is a concerned citizen who bring this action on behalf of tens of millions of Americans to address the conspiracy involving Facebook, Inc. ("Facebook") that has led to the intentional, massive exfiltration of personal information later used, unbeknownst to Facebook users, to serve up targeted political messages.

2. Although Facebook's *publicly*-proclaimed purpose "is to build useful and engaging products that enable people to connect and share with friends and family through mobile devices, personal computers, and other surfaces,"[1] Facebook's true, undisclosed purpose is to amass personal data from its users. Facebook operates to monetize the vast trove of its users' private data by, in part, laundering the data through app developers, who not only pay Facebook to place advertising on its platform, but also use the data they obtain to develop targeted advertising placed by others on Facebook's platform. As such, the true customers of Facebook are the developers and advertisers who benefit from the aggregation of Facebook users' data and the deployment of "an algorithmically-ranked series of stories and advertisements individualized for each person."[2] And Facebook users, rather than being the customers of Facebook, are in

[1] *See* Facebook Inc.'s 2017 Form 10-K at p. 5.
[2] *Id.*.

essence the product Facebook sells to its advertisers.

3. Facebook induces its users into giving up their most personal and private information on the Facebook platform, through its false promises to keep their information private, but then surreptitiously provides that information to third parties in order to generate advertising revenue. The private, personal information held by Facebook is so detailed that the company is able to target advertisements "by location, demographics, likes, keywords, and any other information we receive or can tell about you and other users."[3]

4. Facebook allowed Cambridge Analytica and other third-party app developers access to this highly-personal user data in two ways. First, app developers could gather Facebook users' data directly from the app user. In addition, Facebook provided Cambridge Analytica and other app developers "friends' permission" whereby the same data obtained from the app user could be collected from the app user's Facebook *friends*. Facebook implemented "friends' permission" with no safeguards: the Facebook "friends" did not know of the app, had no agreement with the app, and had never consented to having their data collected by the app.[4] Once the data was collected by Cambridge Analytica and other developers, Facebook exercised no control over how the data was used. As demonstrated by the facts alleged herein, Facebook actively encouraged the use of this data for targeted political and commercial advertising.

5. In 2014, Facebook and Cambridge Analytica agreed to deploy the "friends' permission" to allow Cambridge Analytica to obtain the personal information of more than 50 million Facebook users in the United States. The nature of this information, including interests, likes, location, political affiliation, relationships, religion, photos, videos and more,[5] is of a profoundly personal nature. Cambridge Analytica utilized this information to identify persons as targets for political advertisements, the content of which could be tailored to the targeted persons,

---

[3] *See* Data Use Policy, IV. How Advertising and Sponsored Stories Work, Facebook (updated Dec. 11, 2012), ¶¶ 43, 62, available at https://www.scribd.com/document/191118234/Facebook-2.

[4] *See* https://techcrunch.com/2015/04/28/facebook-api-shut-down/.

[5] The personal information obtained by Cambridge Analytica includes at least the following data sets: about me, actions, activities, birthday, check-ins, education history, events, games activity, groups, hometown, interests, likes, location, notes online presence, photo and video tags, photos, questions, relationship details, relationships, religion, politics, status, subscriptions, website and work history.

as informed by their personal data that Facebook provided to Cambridge Analytica.

6. The Cambridge Analytica affair is not an isolated incident but simply a high-profile exemplar. Facebook's agreements with thousands of app developers to collect and disseminate to third parties of Facebook user data was a years-long conspiracy. During the relevant period, as confirmed by a former Facebook employee, Facebook allowed thousands upon thousands of app developers similar access to user data, without user consent. As one lawmaker noted – "I'm sure there are other Cambridge Analytica's out there. Facebook isn't just a company, it is so powerful it is like a country."[6]

II. THE PARTIES

1. Plaintiff Danielle Reninger is a resident of Will County, Illinois. She established a Facebook account in or around April 2007, and has maintained her account to present day.

2. Defendant Facebook, Inc. ("Facebook") is an American corporation, headquartered in Menlo Park, California, and incorporated under the laws of the State of Delaware. Facebook owns and operates an online social networking website that allows its users to communicate with each other through the sharing of text, photograph, and video.

III. JURISDICTION

3. Pursuant to 28 U.S.C. § 1331, this Court has original subject matter jurisdiction over the claims of Plaintiff and the Class that arise under the Stored Communications Act, 18 U.S.C. §§ 2701 *et seq.*

4. Further, this Court has subject matter jurisdiction over this putative nationwide class action pursuant to 28 U.S.C. § 1332, as amended by the Class Action Fairness Act of 2005 ("CAFA"), because the matter in controversy exceeds $5,000,000.00, exclusive of interest and costs, and is a class action in which members of the Class are citizens of states

[6] *See* https://www.nytimes.com/2018/03/26/technology/ftc-facebook-investigation-cambridge- analytica.html.

different than Defendant. See 28 U.S.C. § 1332(d)(2)(A). Therefore, both elements of diversity jurisdiction under CAFA are present, and this Court has jurisdiction.

5. This Court has personal jurisdiction over Facebook because Facebook conducts substantial business throughout the State of Illinois and Will County.

IV. FACTUAL BACKGROUND

A. Facebook's Data Aggregation and Its Effects on Millions of Individuals

6. With over 2 billion users accessing this service on a monthly basis, Facebook is the world's largest social media company.[7]

7. As information is shared by these billions of unique users, Facebook is provided with sophisticated, exceedingly detailed data profiles. The most revealing data points from these profiles are drawn from observations of the things user's "like" on Facebook (i.e., the instances in which they click a "like" button in association with pages or posts on the Facebook platform). Research from 2013 presented in the Proceedings of the National Academy of Sciences indicated that Facebook data (namely, "likes") contained a rich trove for predicting and manipulating user behavior, even with unlikely correlations:

> A few dozen "likes" can give a strong prediction of which party a user will vote for, reveal their gender and whether their partner is likely to be a man or woman, provide powerful clues about whether their parents stayed together throughout their childhood and predict their vulnerability to substance abuse. And it can do all this without an need for delving into personal messages, posts, status updates, photos or all the other information Facebook holds….[P]sychologyresearchers showed that far more complex traits could be deduced from patterns invisible to a human observer scanning through profiles. Just a few apparently random "likes" could form the basis for disturbingly complex character assessments.[8]

8. For instance, by analyzing aggregated data, the researchers found that when

[7] *See* https://techcrunch.com/2017/06/27/facebook-2-billion-users/..

[8] https://www.theguardian.com/technology/2018/mar/17/facebook-cambridge-analytica-kogan- data-algorithm.

users liked "curly fries" or Sephora cosmetics, there was a correlation to intelligence. Hello Kitty likes, in turn, betrayed political views. "Being confused after waking up from naps" was linked to sexuality.[9]

9. However, Facebook is able to observe – and record – far more than what an individual "likes" on its social media platform. Facebook users also provide the company fine-grained and highly-detailed data points through their other interactions with Facebook, including their age, location, political and religious affiliations, relationship status, and personality traits.

10. Ultimately, the researchers involved in the study of Facebook data points and their correlative predictive value "saw the dystopian potential of the study," warning that "'[t]he predictability of individual attributes from [Facebook's] digital records of [behavior] may have considerable negative implications, because it can easily be applied to large numbers of people without their individual consent and without them noticing.'"[10]

11. These highly-personal, highly-revealing data points were the precise types of information that Facebook offered third party developers, without vetting or follow up, and without authorization of users.

B. Facebook Allowed Developers Access to User Data, With Minimal Limitations and No Follow-Up

12. In 2007, Facebook decided to open access to its so-called social graph — the web of friend connections, "likes" and other Facebook activity that knit users together.[11]

13. Until mid-2014, Facebook allowed third-party app developers access to user data in two ways. First, the app developer could gather Facebook data – including status updates, check-ins, location, and interests – from the app user. But more surprisingly, the app

[9] *Id.*
[10] *Id.*
[11] *See* https://www.wsj.com/articles/facebooks-lax-data-policies-led-to-cambridge-analytica- crisis-1521590720?mg=prod/accounts-wsj.

developer could gather those same data points from the user's *Facebook friends*, despite the fact that those individuals did not know of the app, had no agreement with the app, and had never consented to having their data collected by the app.[12]

14. As discussed in greater detail below, the "friends permission" functionality was implemented with no safeguards or oversight. Once the data was collected by a developer, Facebook had no control over how it was used, did not conduct any follow-up, and only berated developers when reports of their misuse of data came to light publicly.

1. Facebook Willingly Provided Millions of Users' Data to Cambridge Analytica and Other Third Parties.

15. In early 2014, Cambridge Analytica approached scientists at Cambridge University's Psychometrics Centre. Researchers there had developed a technique to map personality traits based on what people had liked on Facebook. The researchers paid users small sums to take a personality quiz and download an app, which would scrape private information from users' profiles as well as the profiles of their friends. Scientists at the Psychometrics Centre said that their data set and their approach could reveal more about a person than their parents or romantic partners knew.[13]

16. As described below, Facebook permitted such activity via its "friends permission" functionality.

17. The Psychometrics Centre declined to work with Cambridge Analytica, but Defendant was undeterred, and found another researcher at Cambridge – Aleksandr Kogan – who possessed an understanding of the data-scraping functionality of the Centre's app and was therefore able to build his own version of the app, "thisisyourdigitallife," under the auspices of a company he formed along with fellow research Joseph Chancellor, Global Science Research ("GSR").

18. Global Science Research deployed the thisisyourdigitallife app in June 2014 to

[12] *See* https://techcrunch.com/2015/04/28/facebook-api-shut-down/.
[13] *See* https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html.

begin harvesting its own set of data. In representations to both Facebook and users, the Company claimed that it was collecting information for academic purposes. Kogan assured the app users their Facebook data would "only be used for research purposes" and remain "anonymous and safe."[14]

19. Facebook did not verify Global Science Research's claims. In reality, Kogan's aim was to get as close to every US Facebook user into its dataset as possible, for Cambridge Analytica's commercial use.[15]

20. Approximately 270,000 Facebook users downloaded the thisisyourdigitallife app and took the corresponding survey. From those 270,000 users – and through Facebook's API – Global Science Research then culled over 50 million raw profiles of Facebook users.

21. The scale of the data collection Cambridge Analytica paid for was so large it triggered an automatic shutdown of the app's ability to harvest profiles. But Kogan told a colleague he "spoke with an engineer" at Facebook to get the restriction lifted and, within a day or two (and no investigation on the part of Facebook), work resumed.[16]

22. Of the 50 million profiles collected, roughly 30 million contained enough information – in the form of demographic data including names, locations, birthdays, genders, as well as their Facebook "likes", which offer a range of personal insights as discussed above – for Global Science Research to build "psychographic profiles," which the Company then provided to Cambridge Analytica.

23. The purpose of these profiles was to manipulate the subjects at issue, typically through targeted advertising or other social media messaging. Christopher Wylie, the former Cambridge Analytica employee who oversaw the production of the 50-million-user-profile

---

[14] *See* https://www.theguardian.com/us-news/2015/dec/11/senator-ted-cruz-president-campaign-facebook-user-data.

[15] *Id.*

[16] *See* https://www.theguardian.com/technology/2018/mar/17/facebook-cambridge-analytica-kogan-data-algorithm.

dataset and who has since turned whistleblower, stated: "We exploited Facebook to harvest millions of people's profiles. And built models to exploit what we knew about them and target their inner demons. That was the basis the entire company was built on."[17]

24. Cambridge Analytica now had a database of millions of US voters that had its own algorithm to scan them, identifying likely political persuasions and personality traits.[18] They could then decide who to target and craft their messages that was likely to appeal to them for those individuals – a political approach known as "micro-targeting."[19]

25. Cambridge Analytica and SCL used the algorithm to analyze individual Facebook profiles and determine personality traits linked to voting behavior. The algorithm and database together made a powerful political tool. It allowed a campaign – such as the Cruz and Trump presidential campaigns, as discussed below – to identify possible swing voters and craft messages more likely to resonate.

26. Cambridge Analytica and SCL covered the costs of Global Science Research's efforts – totaling over $800,000 – and allowed Kogan and Chancellor to keep a copy of all data for their own purposes. Documents show Cambridge Analytica and SCL agreed to a contract with GSR, whereby it would pay its data collection costs in order to improve "match rates" against SCL's existing datasets or to enhance GSR's algorithm's "national capacity to profile capacity of American citizens."[20]

27. A contract between Cambridge Analytica and GSR describes the objective of the data harvesting as follows: "The ultimate product of the training set is creating a 'gold

---

[17] *See* https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election.

[18] The Facebook data was used to generate sophisticated models of each of their personalities using the so-called "big five" personality traits and characteristics – openness, conscientiousness, extraversion, agreeableness, neuroticism (known as the OCEAN scale). (*See* https://www.theguardian.com/us-news/2015/dec/11/senator-ted-cruz-president-campaign- facebook-user-data).

[19] *See* https://www.theguardian.com/technology/2018/mar/17/facebook-cambridge-analytica-kogan-data-algorithm.

[20] *See* https://www.theguardian.com/us-news/2015/dec/11/senator-ted-cruz-president-campaign-facebook-user-data.

standard' of understanding personality from Facebook profile information." The contract promises to create a database of 2 million "matched" profiles, identifiable and tied to electoral registers, across 11 states,[21] but with room to expand much further.

2. Plaintiff and Class Members Did Not Consent to Having Their Data Harvested by Unknown Third-Party Developers.

28. None of those 50 million people whose data was harvested – beyond the 270,000 who downloaded the thisisyourdigitallife app, at absolute most – consented to have their data obtained or to have their "psychographic profiles" created.

29. In response to the instant, growing scandal, Facebook initially claimed that users consented to third-party apps being able to collect their data, via their friends' act of downloading the app and nothing more,[22] describing Kogan's and GSR's acquisition of data as having been done "in a legitimate way and through the proper channels that governed all developers on Facebook at that time."[23] This is incorrect, however. Nothing in Facebook's Statement of Rights and Responsibilities ("SRR") or its Privacy Policy (the documents that form the agreement between Facebook and its users) can be read to have obtained users' consent to *any* of Kogan's and GSR's practices. The applicable portions of the SRR are as follows:

> **2. Sharing Your Content and Information**
>
> You own all of the content and information you post on Facebook, and you can control how it is shared through your privacy and application settings. In addition:
>
> ...
>
> When you use an application, the application may ask for your permission to access your content and information as well as content and information that others have shared with you. We require applications to respect your privacy, and your agreement with that application will control how the

[21] The states are Arkansas, Colorado, Florida, Iowa, Louisiana, Nevada, New Hampshire, North Carolina, Oregon, South Carolina, and West Virginia (*See* https://www.theguardian.com/technology/2018/mar/17/facebook-cambridge-analytica-kogan- data-algorithm).

[22] *See* https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html.

[23] *See* https://newsroom.fb.com/news/2018/03/suspending-cambridge-analytica/.

> application can use, store, and transfer that content and information. (To learn more about Platform, including how you can control what information other people may share with applications, read our Data Use Policy and Platform Page.)

30. Indeed, the SRR affirmatively *obligates* parties using the platform to respect the privacy rights of users:

> **5. Protecting Other People's Rights**
>
> We respect other people's rights, and expect you to do the same.
>
> ...
>
> *If you collect information from users, you will: obtain their consent, make it clear you (and not Facebook) are the one collecting their information, and post a privacy policy explaining what information you collect and how you will use it.*

(italics and underline added)

31. While Facebook's Privacy Policy *does* address the phenomenon of third-party apps being able to acquire user information via that user's friends, Facebook's statement on the matter is patently misleading and describes a scenario entirely different from what Facebook now claims users consented to:

> **Controlling what is shared when the people you share with use applications**
>
> *...If an application asks permission from someone else to access your information, the application will be allowed to use that information only in connection with the person that gave the permission, and no one else.*
>
> For example, some apps use information such as your friends list, to personalize your experience or show you which of your friends use that particular app.

(italics and underline added)

32. These examples are far afield of the full extent of the "friends permission" functionality – including the use of that functionality that was sanctioned by Facebook. Accordingly, Facebook is patently wrong when it suggests that users consented or otherwise authorized *any* of the conduct at issue.

33. The trove of data about a user's friends to developers was exceedingly detailed. The

exfiltrated information appears to relate to virtually every aspect of a person's life as embodied on Facebook: their birthday, their hometown, their religious and political affiliations, their work history, and also highly personal data such as location check-ins, and even the friends' photos and videos.[24] On information and belief, the friends' permission likely allowed access to data of Facebook users that beyond that publicly shared by the users.

3. Cambridge Analytica and SCL Peddled Their Illicit Data Set to 2016 GOP Presidential Candidates, Among Others.

34. During the 2016 Republican Presidential Primary, Ted Cruz's campaign paid Cambridge Analytica $5.8 million between July 2015 and June 2016. The Cruz campaign worked with the firm on "voter ID targeting" and "voter modeling"[25] – utilizing the precise data harvested from Facebook.

35. During this time Cambridge Analytica also worked for the Ben Carson campaign, which paid $220,000 for access to the Facebook data set and attendant micro-targeting opportunities it allowed.[26]

36. Following Cruz's and Carson's loss to Donald Trump in the GOP primary, the Trump campaign contracted with Cambridge Analytica for similar services, harnessing the illicitly-acquired Facebook user data in its voter-targeting efforts. Under the guidance of Brad Parscale, the Trump campaign's digital director in 2016, Cambridge Analytica performed a variety of services, former campaign officials said. That included designing target audiences for digital ads and fund-raising appeals, modeling voter turnout, buying $5 million in television ads and determining where Mr. Trump should travel to best drum up support.[27]

4. Facebook "Discovered" the Unauthorized Acquisition of User Data in 2015, Sent a Letter Requesting the Destruction of the Data, Made No Effort to Confirm the Data's Destruction, and Chose Not to Tell Affected Users.

[24] *See* http://www.businessinsider.com/what-data-did-cambridge-analytica-have-access-to-from-facebook-2018-3.
[25] *See* http://thehill.com/blogs/blog-briefing-room/news/379280-cruz-says-cambridge-analytica- claimed-practices-were-legitimate.
[26] *See* https://www.theguardian.com/us-news/2015/dec/11/senator-ted-cruz-president-campaign-facebook-user-data.
[27] *See* https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html.

37. As discussed above, in late 2015, news reports surfaced describing Cambridge Analytica's use of Facebook user data in Ted Cruz's presidential campaign. The reports tookspecific issue with "the surreptitious, commodified Facebook data," acquired by GSR under false pretenses and laundered through SCL and Cambridge Analytica for purposes of political manipulation.[28]

38. In response to this report, Facebook stated it was "carefully investigating this situation" regarding the use of user data by the Cruz campaign. A Facebook spokesman stated "misleading people or misusing their information is a direct violation of our policies and we will take swift action against companies that do, including banning those companies from Facebook and requiring them to destroy all improperly collected data."[29]

39. Without publicly acknowledging the extent of the data they allowed to be exfiltrated, Facebook, in a superficial effort to appear to be taking action to protect user's privacy, purported to seek to secure the information obtained by SCL/Cambridge Analytica/GSR. These efforts continued as recently as August 2016. That month, lawyers for the social network reached out to Cambridge Analytica contractors. "This data was obtained and used without permission," said a letter that was obtained by the New York Times. "It cannot be used legitimately in the future and must be deleted immediately."[30]

40. A Deputy General Counsel for Facebook further represented that "SCL Group and Cambridge Analytica certified to us that they destroyed the data in question."[31]

41. However, as described by whistleblower Christopher Wylie Facebook's "diligence" was farcical: "[L]iterally all I had to do was tick a box and sign it and send it back, and that was it . . . Facebook made zero effort to get the data back." Further, there were multiple copies of the data set, and it had already been emailed in unencrypted files.[32]

---

[28] *See* https://www.theguardian.com/us-news/2015/dec/11/senator-ted-cruz-president-campaign- facebook-user-data.
[29] *Id.*
[30] *See* https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump- campaign.html.
[31] *Id.*
[32] *See* https://www.theguardian.com/news/2018/mar/17/data-war-whistleblower-christopher- wylie-faceook-nix-bannon-trump.

42. Indeed, rather than conducting a meaningful investigation into the practices of Cambridge Analytica and SCL, Facebook effectively co-opted the fruits of the data exfiltration: Joseph Chancellor, one of Kogan's co-owners of Global Science Research and co-developers of the thisisyourdigitallife app (and co-owner of its attendant data set), currently works for Facebook on the "User Experience Research Team."[33] According to a Facebook spokesperson, "[t]he work that he did previously has no bearing on the work that he does at Facebook."[34] However, his research appears to align precisely with the unlawful work he did under the banner of GSR, "examin[ing] happiness, emotions, social influences, and positive character traits."[35]

5. Cambridge Analytica Continues to Use Its Ill-Gotten Personal Data.

43. Despite Cambridge Analytica's representations to Facebook that it deleted the 50- million-user data set – which destruction Facebook failed to verify – Cambridge Analytica employees claim that the data "formed the backbone of the company's operations in the 2016 presidential election."[36] Indeed, copies of the data still remain beyond Facebook's control. Reporters for the New York Times viewed a set of raw data from the profiles Cambridge Analytica obtained, and a former employee said that he had recently seen hundreds of gigabytes on Cambridge servers, and that said files were not encrypted.

6. The Injury to Class Members Continues to This Day: A Whistleblower Reveals That Illicit Data Collection Was Common Across All Developers, and That Facebook Knew This and Did Nothing.

44. The unlawful data harvesting operation employed by GSR, SCL, and Cambridge Analytica is not an anomaly on Facebook's platform. Instead, it is common.

45. Following reporting on Cambridge Analytica's siphoning of user data, a former Facebook employee – Sandy Parakilas, the platform operations manager at Facebook between

---

[33] *See* https://research.fb.com/people/chancellor-joseph/.
[34] *See* https://theintercept.com/2017/03/30/facebook-failed-to-protect-30-million-users-from- having-their-data-harvested-by-trump-campaign-affiliate/.
[35] *See* https://research.fb.com/people/chancellor-joseph/.
[36] *See* https://www.nytimes.com/2018/03/19/opinion/facebook-cambridge-analytica.html.

2011 and 2012 – told the Guardian he warned senior executives at the company that its lax approach to data protection risked a major privacy event. "My concerns were that all of the data that left Facebook servers to developers could not be monitored by Facebook, so we had no idea what developers were doing with the data," he said.[37]

46. Parakilas, whose job was to investigate exfiltration of data by developers similar to the one later perpetuated by Global Science Research, said the slew of recent disclosures: "It has been painful watching . . . because I know that they could have prevented it."[38]

47. Asked what kind of control Facebook exercised over the data given to outside developers, he replied: "Zero. Absolutely none. Once the data left Facebook servers there was not any control, and there was no insight into what was going on."[39]

48. Parakilas "always assumed there was something of a black market" for Facebook data that had been passed to external developers. However, he said that when he told other executives the company should proactively "audit developers directly and see what's going on with the data"[40] he was actively discouraged from doing so.

49. He said one Facebook executive advised him against investigating how the data was being used, warning him: ***"Do you really want to see what you'll find?"***[41] Parakilas interpreted the comment to mean that "Facebook [believed it] was in a stronger legal position if it didn't know about the abuse that was happening…They felt that it was better not to know. I found that utterly shocking and horrifying."[42]

50. Parakilas said he lobbied internally at Facebook for "a more rigorous approach" to enforcing data protection but was rebuffed. His warnings included a PowerPoint presentation he delivered to senior executives in mid-2012 "that included a map of the vulnerabilities for user data

---

[37] *See* https://www.theguardian.com/news/2018/mar/20/facebook-data-cambridge-analytica- sandy-parakilas.
[38] *Id.*
[39] *Id.*
[40] *Id.*
[41] *Id.*
[42] *Id.*

on Facebook's platform…I included the protective measures that we had tried to put in place, where we were exposed, and the kinds of bad actors who might do malicious things with the data," he said. "On the list of bad actors, I included foreign state actors and data brokers."

51. However, Facebook refused to address the potentially widespread data misuse. In Parakilas's time at the company, he "didn't see them conduct a single audit of a developer's systems." In fact, Facebook's "enforcement" efforts were a sham; as the facts have borne out, even when Facebook was confronted with *indisputable evidence* of data misuse, its policy was to ask the bad actor to check a box, and nothing more.

52. The likelihood of banning a developer for data misuse was effectively nil. Parakilas was told that any decision to ban an app required the personal approval of the chief executive, Mark Zuckerberg.

53. Facebook recognized the value in nonexistent oversight of developers' access of user data, and in fact actively encouraged the exfiltration of "friends permission" user data. From 2007 until its cessation in mid-2014, the "friends permission" functionality allowed tens of thousands of developers to access user data without the consent of those users. Academic research from 2010, based on an analysis of 1,800 Facebooks apps, concluded that around 11% of third-party developers requested data belonging to friends of users. If those figures are extrapolated, tens of thousands of apps, if not more, were likely to have systematically culled "private and personally identifiable" data belonging to hundreds of millions of users.

54. Facebook's incentive to offer up user data in this manner was twofold: first, it enticed developers to create third party content that kept users engaged on Facebook; second, Facebook took a 30% cut of any payments made to those developers' apps.[43]

55. Ultimately, it was not concern over user privacy that ended the "friends permission" policy, but rather economic self-interest. Facebook feared that *too much* user data was being exported by developers *off the Facebook platform*, and thus some of the largest apps – with

[43] *Id.*

the greatest capacity to siphon user data without consent – had become able to create their own social graphs and thus position themselves as competitors to Facebook.[44]

56. However, before turning off the firehose of personal user data in 2014, Parakilas estimates that hundreds of millions of users ("a majority of Facebook users") have had their data exfiltrated, without their consent, by unknown third parties. These data are being used to this day, with no oversight and in direct violation of the most basic autonomy and privacy rights of the individuals who have been – and continue to be – profiled.

57. Nor was Parakilas the only Facebook employee who sought greater protections for users (and who was subsequently overruled by executives more concerned with valuing profit over security). After the news of the Cambridge Analytica scandal, Facebook's Chief Security Officer, Alex Stamos, is said to be resigning, following a series of clashes with other executives over Facebook's infiltration by Russian actors in the 2016 election. Tellingly, he has been overseeing the transfer of his security team to Facebook's product and infrastructure divisions. His group, which once had 120 people, now has three.[45]

58. Facebook's malfeasance in the handling of its users' personal data has dealt users profound harm. As one commentator encapsulates the issue:

> If Facebook failed to understand that this data could be used in dangerous ways, that it shouldn't have let anyone harvest data in this manner and that a third-party ticking a box on a form wouldn't free the company from responsibility, it had no business collecting anyone's data in the first place. But the vast infrastructure Facebook has built to obtain data, and its consequent half-a-trillion-dollar market capitalization, suggest that the company knows all too well the value of this kind of vast data surveillance.[46]

CLASS ALLEGATIONS

59. Plaintiff brings this nationwide class action, pursuant to Rule 23(b)(2), 23(b)(3) and 23(c)(4) of the Federal Rules of Civil Procedure, individually and on behalf of all members of

---

[44] *Id.*

[45] *See* https://www.nytimes.com/2018/03/19/technology/facebook-alex-stamos.html.

[46] *See* https://www.nytimes.com/2018/03/19/opinion/facebook-cambridge-analytica.html.

the following Class:

> All persons who registered for Facebook accounts in the United States and whose Personal Information was obtained by app developers through the "friends permission" functionality.

60. Excluded from the Class are the following individuals and/or entities: Facebook and its parents, subsidiaries, affiliates, officers and directors, current or former employees, and any entity in which Facebook has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

61. Plaintiff reserves the right to modify or amend the definition of the proposed Class before the Court determines whether certification is appropriate.

62. The Class is so numerous that joinder of all members is impracticable. Upon information and belief, there are more than 166 million Facebook account holders in the United States. As discussed above, the number of individuals whose user profiles were surreptitiously exfiltrated by third party apps is likely in the tens or even hundreds of millions and is identifiable and ascertainable based on Facebook's records.

63. There are questions of law or fact common to the Class. These questions include, but are not limited to, the following:

a. Whether Facebook defrauded users by representing that it would safeguard Plaintiff's and Class members' Personal Information and not disclose it without consent;

b. Whether Defendant improperly obtained and disclosed Plaintiff's and Class members' Personal Information without authorization or in excess of any authorization;

c. Whether Defendant conspired and/or engaged in a common enterprise with respect to the improper collection and exfiltration of Plaintiff's and Class members' Personal Information;

d. Whether Defendant owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, safeguarding, and/or obtaining their

Personal Information;

e. Whether Defendant breached a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, safeguarding, and/or obtaining their Personal Information;

f. Whether Defendant's conduct violated the Stored Communications Act, 18 U.S.C. §§ 2701, et seq.;

g. Whether Defendant's conduct violated Plaintiff's and Class Members' common law right to privacy;

h. Whether Plaintiff and the Class are entitled to equitable relief, including, but not limited to, injunctive relief and restitution.

i. Whether Plaintiff and the other Class members are entitled to actual, statutory, or other forms of damages, and other monetary relief.

64. Plaintiff's claims are typical of the claims of the class. Regardless of the privacy of their Facebook accounts, Plaintiff and Class members did not consent to the data exfiltration, which comprises the basis for this suit. Plaintiff and Class members are entitled to declaratory relief, statutory damages, restitution, and injunctive relief as a result of the conduct complained of herein. Moreover, upon information and belief, the conduct complained of herein systemic. Thus, the representative Plaintiff, like all other Class members, face substantial risk me injury in the future. The factual basis of Facebook's conduct is common to all Class s and represents a common thread of conduct resulting in injury to all members of the Plaintiff have suffered the harm alleged and have no interests antagonistic to any other ember.

65. Plaintiff will fairly and adequately protect the interests of the Class. Plaintiff does not conflict with the interests of the Class members. Furthermore, Plaintiff has competent counsel experienced in class action litigation. Plaintiff's counsel will fairly and adequately protect and represent the interests of the Class. Fed. R. Civ. P. 23(a)(4) and 23(g) are satisfied.

66. Plaintiff asserts that pursuant to Fed. R. Civ. P. 23(b)(3), questions of law or fact common to the Class members predominate over any questions affecting only individual members.

67. A class action is superior to other available methods for the fair and efficient

adjudication of this controversy. Arguably no Class member could afford to seek legal redress individually for the claims alleged herein. Therefore, absent a class action, the Class members will continue to suffer losses and Facebook's misconduct will proceed without remedy.

68. Even if Class members themselves could afford such individual litigation, the court system could not. Given the complex legal and factual issues involved and considering that the Class could number in the tens of millions or greater, individualized litigation would significantly increase the delay and expense to all parties and to the Court. Individualized litigation would also create the potential for inconsistent or contradictory rulings. By contrast, a class action presents far fewer management difficulties, allows claims to be heard which may otherwise go unheard because of the relative expense of bringing individual lawsuits, and provides the benefits of adjudication, economies of scale and comprehensive supervision by a single court.

69. Further, Defendant has acted or refused to act on grounds generally applicable to the Class and, accordingly, final injunctive or corresponding declaratory relief with regard to the members of the Class as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

70. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Facebook knew about and/or encouraged the improper collection of Personal Information by app developers;

b. Whether Facebook's representations that they would secure and not disclose without consent the Personal Information of Plaintiff and members of the classes were facts that reasonable persons could be expected to rely upon when deciding whether to use Facebook's services;

c. Whether Facebook misrepresented the safety of its systems and services, specifically the security thereof, and their ability and willingness to safely store Plaintiff's and Class members' Personal Information;

d. Whether Facebook failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;

e. Whether Defendant's acts, omissions, misrepresentations, and practices were and are likely to deceive consumers;

CAUSES OF ACTION

COUNT ONE
(Violations of the Stored Communications Act, 18 U.S.C. §§ 2701, *et seq.*)

71. Plaintiff adopt and incorporate each and every allegation of this complaint as if stated fully herein.

72. Plaintiff, individually and on behalf of Class members, assert violations of 18 U.S.C. §§ 2702(a) for Facebook's unlawful disclosure/divulging of the content of Plaintiff's and Class members' communications to third parties, including but not limited to SCL, Cambridge Analytica, Aleksandr Kogan, and GSR.

73. The Stored Communications Act prohibits a person from intentionally accessing without (or in excess of) authorization a facility through which an electronic communications service is provided and thereby obtaining an electronic communication while it is in "electronic storage."

74. The SCA defines "electronic storage" as "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and any storage of such communication by an electronic communication service for purposes of backup protection of such communication."

75. The servers Facebook uses to provide its electronic communications service to Facebook users are a "facility" within the meaning of the SCA.

76. Facebook is a "person" within the meaning of the SCA.

77. Facebook's provision of 'users' personal data with third parties as alleged herein exceeded any authorization from any party to the personal data at issue.

78. Because of the architecture of Facebook's servers, the sharing of personal data among Facebook users results in and constitutes interstate data transmissions.

79. Pursuant to 18 U.S.C. § 2707(c), Plaintiff and Class members are entitled to:

i. minimum statutory damages of $1,000 per person;

ii. punitive damages;

iii. costs; and

iv. reasonable attorneys' fees.

COUNT TWO
(Violations of the Illinois Consumer Fraud and Deceptive Practices Act)

80. Plaintiff adopts and incorporate each and every allegation of this complaint as if stated fully herein.

81. Defendant's conduct as alleged herein constitutes unfair, unlawful, or fraudulent business acts or practices as proscribed by the Illinois Consumer Fraud and Deceptive Practices Act ("ICFDPA").

82. Defendant's conduct constitutes "unlawful" business acts or practices by virtue of Defendant's violation of the Stored Communications Act, 18 U.S.C. §§ 2701, *et seq.*; and ICFDPA.

83. Plaintiff and Class members reasonably relied on representations from Facebook that third parties could not access personal data absent (including representations in Facebook's operative terms of service that *omitted* disclosure of the data that could be acquired, without consent, via the "friends permission" functionality). Similarly, Cambridge Analytica, SCL Group, GSR, and Kogan used patent misrepresentations in order to obtain Plaintiff's and Class members' data through the "thisisyourdigitallife" app, representing that the app sought data for academic research purposes – when in fact the app harvested data (1) from the *friends* of the app's users (without their consent) and (2) expressly for political targeting purposes. All of the above-described activity constitutes "fraudulent" business acts or practices.

84. Plaintiff and Class members have an interest in controlling the disposition and

dissemination of their private data, stemming from traditional privacy and autonomy rights enshrined in centuries of legal tradition. Contrary to Plaintiff's and Class members' interests, each Defendant exercised control over the content of Plaintiff's and Class members' personal data, exploiting it for sale and profit without consent. As a result, Defendant's conduct constitutes "unfair" business acts or practices.

85. Plaintiff and Class members have suffered injury in fact and lost money or property as a result of Defendant's business acts or practices.

86. Plaintiff and Class Members seek an order to enjoin Defendant from such unlawful, unfair, and fraudulent business acts or practices, and to restore to Plaintiff and Class Members their interest in money or property that may have been acquired by Defendant by means of unfair competition.

COUNT THREE
(Invasion of Privacy – Intrusion Upon Seclusion)

87. Plaintiff adopt and incorporate each and every allegation of this complaint as if stated fully herein.

88. Plaintiff and Class members have reasonable expectations of privacy in their online behavior on Facebook.

89. The reasonableness of such expectations of privacy is supported by Facebook's unique position to monitor Plaintiff's and Class members' behavior through its access to Plaintiff's and Class members' user data. It is further supported by the surreptitious, highly- technical, and non-intuitive nature of Defendant's collective tracking and exfiltrating of Class members' personal data, via third party apps that Class members did not download, much less provide authorization for such behavior.

90. Defendant intruded on and into Plaintiff's and Class members' solitude, seclusion, or private affairs. Facebook intentionally designed its platform – and established commensurate policies and procedures governing such platform – to enable the exfiltration, without authorization,

of Class members' personal data by third-party apps such as "thisisyourdigitallife." Cambridge Analytica, SCL Group, Kogan, and GSR intentionally availed themselves of Facebook's privacy-invasive measures in order to acquire Class members' personal data without consent.

91. Defendant intruded on and into Plaintiff's and Class members' solitude, seclusion, or private affairs by intentionally facilitating the exfiltration of Class members' personal data to surreptitiously obtain, improperly gain knowledge of, review, and/or retain Plaintiff's and Class members' personal data and activities through the monitoring technologies and policies described herein.

92. These intrusions are highly offensive to a reasonable person. This is evidenced by, *inter alia*, the immense outcry following the revelation of these acts and practices – not only from the public, but also from regulators and legislators. Further, the extent of the intrusion cannot be fully known, as the nature of privacy invasion involves sharing Plaintiff's and Class members' personal information with potentially countless third-parties, known and unknown, for undisclosed and potentially unknowable purposes, in perpetuity. Also supporting the highly offensive nature of Defendant's conduct is the fact that Defendant's principal goal was to surreptitiously monitor Plaintiff and Class members—in one of the most private spaces available to an individual in modern life—and to allow third-parties to do the same.

93. Plaintiff and Class members were harmed by the intrusion into their private affairs as detailed throughout this Complaint.

94. Defendant's actions and conduct complained of herein were a substantial factor in causing the harm suffered by Plaintiff and Class members.

95. As a result of Defendant's actions, Plaintiff and Class members seek injunctive relief, in the form of (1) destruction of all data obtained by Cambridge Analytica; (2) certification by Facebook that no third parties presently are able to access Plaintiff's and Class members' user data without first obtaining express consent; (3) audits, by Facebook, of all third parties who obtained user data through the "friends permissions" feature; (4) notification, by Facebook to Plaintiff and Class members, of each instance in which a third party obtained user data – including

the type of user data – via the "friends permissions" feature; and (5) destruction of all improperly obtained user data of Plaintiff and Class members.

96. As a result of Defendant's actions, Plaintiff and Class members seek nominal and punitive damages in an amount to be determined at trial. Plaintiff and Class members seek punitive damages because Defendant's actions – which were malicious, oppressive, willful – were calculated to injure Plaintiff and made in conscious disregard of Plaintiff's rights. Punitive damages are warranted to deter Defendant from engaging in future misconduct.

COUNT FOUR
(Declaratory Relief Pursuant to 28 U.S.C. §2201)

97. Plaintiff adopt and incorporate each and every allegation of this complaint as if stated fully herein.

98. An actual controversy, over which this Court has jurisdiction, has arisen and now exists between the parties relating to the legal rights and duties of Plaintiff and Defendant for which Plaintiff desires a declaration of rights.

99. Plaintiff contends and Defendant disputes that Defendant, in whole or in part, was authorized by Plaintiff and Class members to acquire user data via the "friends permissions" functionality without the express consent, from each developer, of all users whose personal data was thereby acquired.

100. Plaintiff, on behalf of herself and the Class are entitled to a declaration that Defendant's behavior violated the Stored Communications Act, CIPA, the UCL, and Plaintiff's common law claims.

COUNT FIVE
(Conversion)

101. Plaintiff incorporates the substantive allegations contained in all previous paragraphs as if fully set forth herein.

102. Plaintiff and Class members were the owners and possessors of their private

information. As the result of Defendant's wrongful conduct, Defendant has interfered with the Plaintiff's and Class members' rights to possess and control such property, to which they had a superior right of possession and control at the time of conversion.

103. As a direct and proximate result of Defendant's conduct, Plaintiff and the Class members suffered injury, damage, loss or harm and therefore seek compensatory damages.

104. In converting Plaintiff Private Information, Defendant has acted with malice, oppression and in conscious disregard of the Plaintiff and Class members' rights. Plaintiff, therefore, seeks an award of punitive damages on behalf of the Class

JURY DEMAND

Pursuant to Federal Rule of Civil Procedure 38, Plaintiff, individually and on behalf of the Class they seek to represent, demand a jury on any issue so triable of right by a jury.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and all Class members, request judgment be entered against Defendant and that the Court grant the following:

1. An order determining that this action may be maintained as a class action under Rule 23 of the Federal Rules of Civil Procedure, that Plaintiff is a proper class representative, that Plaintiff's attorneys be appointed Class counsel pursuant to Rule 23(g) of the Federal Rules of Civil Procedure, and that Class notice be promptly issued;

2. Judgment against Defendant for Plaintiff's and Class members' asserted causes of action;

3. Appropriate declaratory relief against Defendant;

4. Preliminary and permanent injunctive relief against Defendant;

5. An award of all applicable statutory damages;

6. An award of reasonable attorney's fees and other litigation costs reasonably incurred; and

7. Any and all relief to which Plaintiff and the Class may be entitled

Dated: June 21, 2018

Respectfully submitted,

POWER ROGERS & SMITH LLP

By: */s/ Todd A. Smith*

Todd A. Smith
tsmith@prslaw.com
Brian LaCien
blacien@prslaw.com
Power Rogers & Smith, LLP
70 W. Madison Street, 55th Floor
Chicago, IL 60602-4212
P: 312-236-9381
F: 312-236-0920

Attorneys for Plaintiff Danielle Reninger